

## UNITED STATES DISTRICT COURT

for the  
District of South Dakota

IN THE MATTER OF THE SEARCH OF: )

INFORMATION ASSOCIATED WITH THE )  
FOLLOWING FACEBOOK USER: )

Karl.koster.75; ESP User ID: )

100002462616167 )

Profile URL: )

http://www.facebook.com/karl.koster.75 )

THAT IS STORED AT PREMISES

CONTROLLED BY FACEBOOK INC.

Case No. 5:20-mj-43

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

SEE "ATTACHMENT A", which is attached to and incorporated in this Application and Affidavit

located in the District of South Dakota, there is now concealed (*identify the person or describe the property to be seized*):

SEE "ATTACHMENT B", which is attached to and incorporated in this Application and Affidavit

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

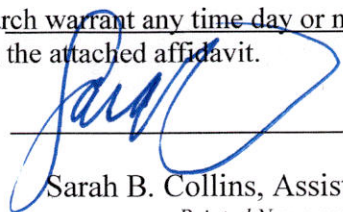
- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☐ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. §§ 2251, 2252, 2252A	Production, Receipt, and Possession of Child Pornography

The application is based on these facts:

- ☒ Continued on the attached affidavit, which is incorporated by reference.  
☐ Delayed notice of \_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.  
☐ Your applicant requests that no notice be given prior to the execution of the search warrant, i.e., "no knock", the basis of which is set forth in the attached affidavit.  
☐ Your applicant requests authorization to serve the search warrant any time day or night pursuant to Fed. R. Crim. P. 41(e)(2)(A)(ii), the basis of which is set forth in the attached affidavit.

  
 Sarah B. Collins, Assistant U.S. Attorney  
*Printed Name and Title*

Sworn to before me and: ☒ signed in my presence.  
☐ submitted, attested to, and acknowledged by reliable electronic means.

Date: 3-4-2020

  
 Judge's signature

City and state: Rapid City, SD

Daneta Wollmann, U.S. Magistrate  
*Printed name and title*

UNITED STATES DISTRICT COURT  
DISTRICT OF SOUTH DAKOTA  
WESTERN DIVISION

IN THE MATTER OF THE SEARCH OF  
INFORMATION ASSOCIATED WITH THE  
FOLLOWING FACEBOOK USER: Karl.koster.75;  
ESP User ID: 100002462616167  
Profile URL:  
<http://www.facebook.com/karl.koster.75>  
THAT IS STORED AT PREMISES CONTROLLED BY  
FACEBOOK INC.

5:20-mj-43

**Filed Under Seal**

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

State of South Dakota    )  
  ) ss  
County of Pennington    )

I, Elliott Harding, Detective with the Rapid City Police Department and currently assigned to the South Dakota Internet Crimes Against Children Taskforce (ICAC), being duly sworn, states as follows:

1. I have been a law enforcement officer since December 1st of 2008. I have received training at the Law Enforcement Training Academy in Pierre, SD, training as a new police officer recruit along with various Police Training Officers and my own experience working in the Patrol Division. I have worked as a Detective in the Criminal Investigations Department beginning April of 2014 and primarily focused on stolen vehicles, pursuits and other general property crimes. During that time, I attended the Reid Technique of Interview and Interrogations. I have worked as a Detective in the Internet Crimes Against Children (ICAC) Task Force since August of 2015. During this time, I have attended classes in regards to on-line ads and undercover chat investigations as

it pertains to child exploitation as well as prostitution/human trafficking. I have also attended classes in regards to the BitTorrent Network as it pertains to the download and sharing of child pornography files. As a Special Assistant Attorney General with State of South Dakota my duties include investigations related to illegal possession and distribution of images containing sexually explicit material, and investigations dealing with illegal activities concerning the Internet or World Wide Web.

2. I have investigated and assisted in the investigation of cases involving the possession, receipt, and distribution of child pornography in violation of federal law to include United States Statues 18 U.S.C. §§ 2251, 2252 and 2252A, involving violations of law involving child pornography. During my law enforcement-career, I have become familiar with the *modus operandi* of persons involved in the illegal production, distribution and possession of child pornography. Based on my experience and training, I am knowledgeable of the various means utilized by individuals who illegally produce, distribute, receive and possess child pornography.

3. I have been informed that 18 U.S.C. §§ 2251, 2252 and 2252A, prohibit the manufacture, distribution, receipt, and possession of child pornography.

4. I make this affidavit in support of an application for a search warrant for information associated with a certain Facebook user ID that is stored at premises owned, maintained, controlled, or operated by Facebook Inc. ("Facebook"), a social networking company headquartered in Menlo Park,

California. The information to be searched is described in the following paragraphs and in Attachments A and B.

5. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Facebook to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the user IDs.

6. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that evidence of violations of 18 U.S.C. § 2252 and 2252A, are present in the following Facebook account (also referred to as SUBJECT ACCOUNT):

Karl.koster.75;

ESP User ID: 100002462616167;

Profile URL: <http://www.facebook.com/karl.koster.75>

There is also probable cause to search the information described in Attachment A for evidence, contraband, or fruits of these crimes, as further described in Attachment B.

#### DEFINITIONS

7. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. *Chat*: as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature



distinguishes chatting from other text-based online communications such as Internet forums and email.

b. *Child Erotica*: as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

c. *Child pornography*: as defined in 18 U.S.C. § 2256(8), is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. *Cloud-based storage service*: as used herein, refers to a publically accessible, online storage provider that collectors of child pornography can use to store and trade child pornography in larger volumes. Users of such a service can share links and associated passwords to their stored files with other traders of child pornography in order to grant access to their collections. Such services allow individuals to easily access these files through a wide variety of electronic devices such as desktop and laptop computers, mobile phones, and tablets, anywhere and at any time. An individual with the password to file stored on a

cloud-based service does not need to be a user of the service to access the file. Access is free and readily available to anyone who has an internet connection.

e. *Computer*: The term “computer” means “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.” See 18 U.S.C. §§ 2256(6) and 1030(e)(1). As used herein, a computer includes a cell phone, smart phone, tablet, and other similar devices capable of accessing the Internet.

f. *Computer Hardware*: The term “computer hardware” means all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices such as video gaming systems, electronic music playing devices, and mobile phones); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, modems, routers, scanners and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

g. *Computer-related documentation*: as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates

how to configure or use computer hardware, computer software, or other related items.

h. *Computer Passwords and Data Security Devices:* The term “computer passwords and data security devices” means information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

i. *Computer-Related Documentation:* The term “computer-related documentation” means written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

j. *Computer Software:* The term “computer software” means digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

k. *Electronic Communication Service* ("ESP"): as defined in 18 U.S.C. § 2510(15), is a provider of any service that gives to users thereof the ability to send or receive wire or electronic communications. For example, "telephone companies and electronic mail companies" generally act as providers of electronic communication services. See S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3568.

l. *Electronic Storage Device*: includes but is not limited to external and internal hard drives, thumb drives, flash drives, SD cards, gaming devices with storage capability, storage discs (CDs and DVDs), cameras, cellular phones, smart phones and phones with photo-taking and/or internet access capabilities, and any "cloud" storage by any provider.

m. *File Transfer Protocol* ("FTP"): as used herein, is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.

n. *Internet*: The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

o. *Internet Connection*: The term "Internet connection" means a connection required for access to the Internet. The connection would generally



be provided by cable, DSL (Digital Subscriber Line), wireless devices, or satellite systems.

p. *Minor*: The term “minor” means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

q. *Records, documents, and materials*: as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

r. *Remote Computing Service* (“RCS”): as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

s. *Short Message Service* (“SMS”): as used herein, is a service used to send text messages to mobile phones. SMS is also often referred to as texting, sending text messages or text messaging. The service allows for short text messages to be sent from one cell phone to another cell phone or from the Web to another cell phone. The term “computer,” as defined in 18 U.S.C. § 1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

t. *Storage Medium*: The term “storage medium” refers to any physical object upon which computer data can be recorded. Examples include hard

disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

u. *Visual Depictions*: “Visual depictions” include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

v. *Wireless Network*: The term “wireless network” means a system of wireless communications in which signals are sent and received via electromagnetic waves such as radio waves. Each person wanting to connect to a wireless network needs a computer, which has a wireless network card that operates on the same frequency. Many wired networks base the security of the network on physical access control, trusting all the users on the local network. However, if wireless access points are connected to the network, anyone in proximity to the network can connect to it. A wireless access point is equipment that connects to the modem and broadcasts a signal. It is possible for an unknown user who has a computer with a wireless access card to access an unencrypted wireless network. Once connected to that network, the user can access any resources available on that network to include other computers or shared Internet connections.

#### **PROBABLE CAUSE**

6. On January 7, 2020, I received CyberTips 60983628 and 61155796 from the National Center for Missing and Exploited Children (NCMEC). The reporting parties were Facebook and Yahoo respectively. The CyberTips were

copied to compact disc under this case report number and stored in ICAC evidence. Below is a brief summary of the information.

**CYBERTIP 60983628**

7. This cybertip contained the following information:

- Reporting ESP: Facebook
- **Incident Information**
  - Incident Type: Child Pornography (possession, manufacture, and distribution)
  - Incident Time: 12-10-2019 04:58:17 UTC
- **Suspect**
  - Name: Karl Koster
  - Mobile Phone: +16058582472 (Verified)
  - Date of Birth: 09-18-1981 Approximate Age: 38
  - Email Address: kosterkarl@yahoo.com (Verified)
  - Screen/User Name: karl.koster.75 ESP User ID: 100002462616167
  - Profile URL: <http://www.facebook.com/karl.koster.75>
- **(SUBJECT ACCOUNT)**
  - IP Address: 2600:1014:b06f:c42c:1938:d518:bd08:214f (Login)
  - 11-30-2019 03:30:16 UTC
  - IP Address: 67.158.42.135 (Other)
  - 12-10-2019 03:57:24 UTC
- Additional Information: Estimated location on December 11, 2019 UTC: Deadwood, South Dakota, US (Not Verified)  
Email: kosterkarl@yahoo.com (Verified)
- This report contains a recent, believed-to-be non-mobile IP address under event type Other.
- **Additional Information Submitted by the Reporting ESP**
  - This report contains additional information about the recipient of the reported content:
  - Recipient(s):
    - First Name: Kristy
    - Last Name: Smith
    - Email: kosterkristy1@gmail.com (Verified)
    - Age: 28
    - DOB: 1991-09-18
    - Gender: Female
    - Profile Url: <http://www.facebook.com/people/Kristy-Smith/100004322865534>
    - Account ID: 100004322865534
    - IP Address: 67.158.42.135

- IP Capture Date: December 10, 2019 at 05:23:38 UTC
- **Uploaded File Information**
  - Number of uploaded files: 2
  - Filename:  
73bffa4tjhs8c8cc79222830\_426638568004705\_2097147065082576896\_n.jpg
  - MD5: 60f74a6fc39786d984dea0e5e5e9687b
  - Submittal ID: 07911e343617de923cb5df9c03abcd36
- Did Reporting ESP view entire contents of uploaded file? Yes
- Did Reporting ESP view the EXIF of uploaded file? (Information Not Provided by Company)
- Were entire contents of uploaded file publicly available? (Information Not Provided by Company)
- Sent in product: Messenger
- File's unique ESP Identifier: 426638564671372
- Uploaded December 10, 2019 at 04:58:17 UTC
- Type: IP Address
- Value: 67.158.42.135
- Event: Upload
- Date/Time: 12-10-2019 04:58:17 UTC
- **Uploaded File Information**
  - Filename:  
83v5mpsdzkkc008s67763403\_2359381157487282\_5293448283518140416\_n.jpg
  - MD5: 441a332150492341245bec02d7f87990
  - Submittal ID: b44535ee82a31bf407749f15fc1f6a57
  - Did Reporting ESP view entire contents of uploaded file? Yes
  - Did Reporting ESP view the EXIF of uploaded file? (Information Not Provided by Company)
  - Were entire contents of uploaded file publicly available? (Information Not Provided by Company)
  - Additional Information: This is the profile picture for the account 10000246261616

**PHOTO OBSERVATIONS FOR CYBERTIP 60983628**

8. I observed 73bffa4tjhs8c8cc79222830\_426638568004705\_2097147065082576896\_n.jpg. The photo showed a girl approximately 9-11 years of age with blond hair. The girl was wearing a red long sleeved shirt, white shoes, gray socks, white and gray undershirt and no pants. The girl's nude vagina was exposed. The girl's hands and torso were tied with white rope which was suspended above her. The girl appeared to be in a storage room of some

type. One box in the storage area appeared to have JAAR-MARKT written on it. In the top left corner, I could see manfredo.fotoplenka.ru, written on the photo.

9. I observed 83v5mpsdzkkc008s67763403\_2359381157487282\_5293448283518140416\_n.jpg. The photo showed a dark colored pickup truck parked outside. Detective Jeremy Stauffacher informed me he had seen the same picture on a cell phone he examined belonging to Karl Koster (9/18/81) during a prior investigation, described below.

**CYBERTIP 61155796**

10. Information contained in this cybertip is as follows:

- **Reporting Electronic Service Provider (ESP):** Yahoo! Inc
- **Incident Information**
  - Incident Type: Child Pornography (possession, manufacture, and distribution)  
Incident Time: 12-13-2019 15:00:12 UTC  
Description of Incident Time: This is the date/time when Oath submitted the CyberTip to NCMEC.
  - **Suspect**
    - Name: Karl Koster  
Phone: 1 6054841348  
Email Address: kosterkarl@yahoo.com  
ESP User ID: 4YJ5HLBMKTYVGXEJTRCKNZ7RFE-yahoo  
Additional Information: Alternate Email:  
kosterkristyl@gmail.com
- **Additional Information Submitted by the Reporting ESP**
  - Platform: Files were transmitted over Yahoo Mail.  
Offense date: 2019/12/12 - 16:34:15  
Recently used IP: 67.158.42.135/2019/12/12 - 16:34:15
- **Uploaded File Information** (image one of four)
  - Number of uploaded files: 4
  - Filename: image.5-1.png
  - MD5: 730a1e1965d393284be5306ea3569d5e  
Submittal ID: b3e585d883348c0bb17c5a0530863da8  
Original Filename Associated with File:  
1576063223763765906286.jpg  
Did Reporting ESP view entire contents of uploaded file? Yes  
Did Reporting ESP view the EXIF of uploaded file?



(Information Not Provided by Company)

Were entire contents of uploaded file publicly available?

(Information Not Provided by Company)

Additional Information: message ID for this upload:

AC89A2FQBoMnXfDRMgro-JyHKg8

- o Additional Information: Upload Date/Time: 2019-12-11 11:21:22

- **Uploaded File Information (image two of four)**

- o Filename: image.6-1.png

- o MD5: 730a1e1965d393284be5306ea3569d5e

Submittal ID: 00280c22ec583b5d87967041024596a3

Original Filename Associated with File:

1576063223763765906286.jpg

Did Reporting ESP view entire contents of uploaded file? Yes

Did Reporting ESP view the EXIF of uploaded file?

(Information Not Provided by Company)

Were entire contents of uploaded file publicly available?

(Information Not Provided by Company)

Additional Information: message ID for this upload:

ACBVwotDY68WXfDRKwa6qOWHokM

- o Additional Information: Upload Date/Time: 2019-12-11 11:21:14

- **Uploaded File Information (image 3 of 4)**

- o Filename: image.7-1.png

- o MD5: 0a6dea3ce4a274b5b7af3f0fe0722fb2

Submittal ID: 30d80463f59e21424ebcb313dcb00d48

- o Original Filename Associated with File:

15760626929362053990695.jpg

Did Reporting ESP view entire contents of uploaded file? Yes

Did Reporting ESP view the EXIF of uploaded file?

(Information Not Provided by Company)

Were entire contents of uploaded file publicly available?

(Information Not Provided by Company)

Additional Information: message ID for this upload:

ALqcJkB9r5iUXfDPHQ5T-KrSlRo

- o Additional Information: Upload Date/Time: 2019-12-11 11:12:29

- **Uploaded File Information (image 4 of 4)**

- o Filename: image.8-1.png

- o MD5: 0a6dea3ce4a274b5b7af3f0fe0722fb2

Submittal ID: 4f7a4e1b8b9eec91f19f39243602bc66

Original Filename Associated with File:

15760626929362053990695.jpg

Did Reporting ESP view entire contents of uploaded file? Yes

Did Reporting ESP view the EXIF of uploaded file?

(Information Not Provided by Company)

Were entire contents of uploaded file publicly available?

(Information Not Provided by Company)

Additional Information: message ID for this upload:

AGXgs0soG1oUXfDPFg2I2HVK-8o

- o Additional Information: Upload Date/Time: 2019-12-11  
11:12:22

**PHOTO OBSERVATIONS FOR CYBERTIP 61155796**

11. I observed image.5-1.png and image.6-1.png. Both images appeared to be duplicates of each other. The picture showed a girl approximately 5-8 years of age with shoulder length dark hair. The girl wore only silver colored sandals. I could the girls nude breast area and nude vagina. The girl was standing in a wooded area. The girl was holding a pair of white underwear with an unknown design. The top left of the picture showed the icon of what appeared to be a nude female of unknown age with the text "ONLINE-LOLITA.com" written underneath the icon.

12. I observed image.7-1.png and image.8-1.png. Both images appeared to be duplicates of each other. The picture showed a girl approximately 5-8 years of age with shoulder length dark hair. The girl was kneeling on a bed with a brown zebra stripe pattern. The girl was smiling at the camera. I could see the girl's nude breast area and nude vagina. In the background, I could see a red stuffed animal which appeared to be a bird. Other stuffed animals could be seen behind the girl, but I could not determine what they were. The headboard of the bed was tan in color.

**IDENTIFYING KARL KOSTER**

13. Local police records showed a Karl Koster (9/18/81) living at 314 Summit St. #70, Belle Fourche, SD. Local records showed Karl's phone number as 605-858-2472 as of 11/18/19. It should be noted the name, date of birth

and phone number in local records matched those listed in the suspect information under CyberTip 60983628.

14. Local records also showed Karl to have the phone number 605-484-1384 as of 1/16/19. This phone number is very similar to the phone number of the suspect provided in CyberTip 61155796 which is 605-484-1348.

15. CyberTip 60983628 described Karl Koster sending, child pornography to Kristy Smith via Facebook Messenger. The CyberTip noted Kristy's email address as kosterkristy1@gmail.com and Kristy's date of birth as 9/18/91. It should be noted Kristy's date of birth is the same as Karl's, but 10 years younger. Detective Stauffacher informed me he had observed pictures of Karl wearing what appeared to be woman's underwear, in a prior investigation described in paragraph 17. I believe Kristy Smith is Karl Koster. Persons engaging in child pornography crimes often send themselves the illicit images utilizing multiple accounts, particularly if he believes his identity is obscured in an account that does not link to his legal name.

16. Koster was previously convicted in Pennington County, South Dakota, for Make/Sale/Posses Child pornography and was sentenced on January 3, 2005 to 5 years' imprisonment on three counts to be served consecutively. He paroled in December, 2010. And has remained on parole since that date.

17. In October, 2019, South Dakota State Parole Agent GP Carmichael brought a phone to ICAC and asked that it be forensically examined. Agent Carmichael indicated the phone belonged to a parolee, Karl Koster. Carmichael indicated that Koster was on parole for a previous conviction for state child

pornography charges. Det. Jeremy Stauffacher conducted an examination in CR: 19-108287. Though he did not find child pornography, he did locate images of young girls and concerning Google searches like, "girls in panties," as well as the identifying images described above in paragraph 15.

18. On February 11, 2020, Parole Officer Jennifer Leighty contacted Det. Stauffacher about examining additional devices. She told him that she was conducting a parole search at the time on Karl Koster and that Koster had been placed in jail on a parole hold. Stauffacher informed Leighty of the ICAC investigation into Koster related to the above-described cybertips and that ICAC was planning to conduct a search on Koster's residence in the near future. Leighty seized twenty-one items of evidence (the SUBJECT DEVICES) pursuant to her parole search and turned them over to ICAC. The items remain in ICAC custody awaiting this search warrant.

19. I reviewed Koster's parole agreement, which he signed on 11/18/10 and 12/1/10. In that agreement, Koster agreed that he and all of his possessions were subject to warrantless searches upon reasonable suspicion by the parole agent or other law enforcement. In the agreement; he was also prohibited from possessing internet capable devices without prior approval of parole and sex offender treatment provider. Of the devices seized by parole on February 11, 2020, multiple were internet capable.

#### **INFORMATION ON FACEBOOK**

20. Facebook owns and operates a free-access social networking website of the same name that can be accessed at <http://www.facebook.com>. Facebook allows individuals to specifically communicate with another person through a

Facebook application called "Messenger." In my training and experience, people who engage in online criminal activity often also utilize Facebook to meet victims and other offenders and to chat. Even if Facebook was not utilized in the chat at issue, there is probable cause to believe there will be evidence regarding the unlawful receipt, distribution and possession of child pornography within the target Facebook account.

21. Facebook owns and operates a free-access social networking website of the same name that can be accessed at <http://www.facebook.com>. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

22. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers (for password retrieval), physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

23. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange



communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

24. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create "lists" of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

25. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host, and guest list. In addition, Facebook users can "check in" to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user's profile page also includes a "Wall," which is a space where the user and his or her "Friends" can

post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

26. Facebook allows users to upload photos and videos, which may include any metadata such as location that the user transmitted when s/he uploaded the photo or video. It also provides users the ability to "tag" (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook's purposes, the photos and videos associated with a user's account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

27. Facebook users can exchange private messages on Facebook with other users. These messages, which are similar to e-mail messages, are sent to the recipient's "Inbox" on Facebook, which also stores copies of messages sent by the recipient, as well as other information. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a Chat feature that allows users to send and receive instant messages through Facebook. These chat communications are stored in the chat history for the account. Facebook also has a Video Calling feature, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

28. If a Facebook user does not want to interact with another user on Facebook, the first user can “block” the second user from seeing his or her account.

29. Facebook has a “like” feature that allows users to give positive feedback or connect to particular pages. Facebook users can “like” Facebook posts or updates, as well as webpages or content on third party (*i.e.*, non-Facebook) websites. Facebook users can also become “fans” of particular Facebook pages.

30. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things. Each Facebook account has an activity log, which is a list of the user’s posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as “liking” a Facebook page or adding someone as a friend. The activity log is visible to the user but people who visit the user’s Facebook page cannot view it.

31. Facebook Notes is a blogging feature available to Facebook users, and it enables users to write and post notes or personal web logs (“blogs”); or to import their blogs from other services, such as Xanga, LiveJournal, and Blogger.

32. The Facebook Gifts feature allows users to send virtual “gifts” to their friends that appear as icons on the recipient’s profile page. Gifts cost money to purchase, and a personalized message can be attached to each gift. Facebook users can also send each other “pokes,” which are free and simply result in a notification to the recipient that he or she has been “poked” by the sender.

33. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

34. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications (“apps”) on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user’s access or use of that application may appear on the user’s profile page. Facebook uses the term “Neoprint” to describe an expanded view of a given user profile. The “Neoprint” for a given user can include the following information from the user’s profile: profile contact information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends’ Facebook user identification numbers; groups and networks of which the user is a member, including the groups’ Facebook group identification numbers; future and past event postings; rejected “Friend” requests; comments; gifts; pokes; tags; and information about the user’s access and use of Facebook applications.

35. Facebook also retains Internet Protocol (“IP”) logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user’s IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

36. Social networking providers like Facebook typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

37. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user's "Neoprint," IP log, stored electronic communications, and other data retained by Facebook, can indicate who has used or controlled the Facebook account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the user accessed



or used the account. For example, as described herein, Facebook logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining, the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, Facebook builds geo-location into some of its services. Geo-location allows, for example, users to "tag" their location in posts and Facebook "friends" to locate each other. This geographic and timeline information may tend to either inculcate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner's state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

38. Therefore, the computers of Facebook are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

**INFORMATION TO BE SEARCHED**  
**AND THINGS TO BE SEIZED**

39. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Facebook to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

**REQUEST/JUSTIFICATION FOR  
ORDER OF NONDISCLOSURE**

40. The United States respectfully applies for an order of nondisclosure to Facebook under 18 U.S.C. § 2705(b) regarding the following account:  
Karl.koster.75;  
ESP User ID: 100002462616167;  
Profile URL: <http://www.facebook.com/karl.koster.75>

41. The United States is seeking this search warrant for user information, including all names, addresses, IP addresses, including historical, telephone numbers, other email addresses, information on length and types of services and any means of payment related to these accounts under the authority given by 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A). Based on § 2703(c)(3), the United States is not required to provide notice to the subscriber. Under § 2705(b), the United States may apply to the court for an order commanding Facebook not to notify the subscriber of the existence of the search warrant. The court may decide what length of time shall apply to the

order of nondisclosure if the court determines the notification to the subscriber could result in one of the five factors listed in the statute, which includes destruction of or tampering with evidence. 18 U.S.C. § 2705(b)(3). The basis for the request is that such disclosure could cause any person with access to the accounts, or any related account or account information, to tamper with or modify the content or account information and thereby destroy or tamper with evidence and otherwise seriously jeopardize the investigation. Especially due to the ease of access to Facebook, its content can be modified by persons with internet access and sufficient account information. As such, the United States respectfully requests this Court enter an order commanding Facebook not to notify the user of the existence of this warrant.

#### **REQUEST FOR SEALING**

42. I further request that the Court order that the matter be sealed until further order of the Court. The matter is an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal the matter because premature disclosure may seriously jeopardize the ongoing investigation.

#### **LIMIT ON SCOPE OF SEARCH**

43. I submit that if during the search, agents find evidence of crimes not set forth in this affidavit, another agent or I will seek a separate warrant.

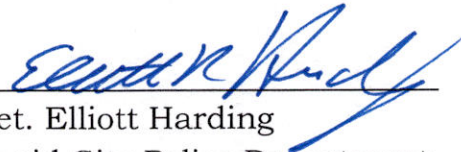
#### **CONCLUSION**

44. Based on the forgoing, I request that the Court issue the proposed search warrant.

45. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A).

46. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

Dated: 3/4/20

  
Det. Elliott Harding  
Rapid City Police Department  
Internet Crimes Against Children  
Taskforce

SUBSCRIBED and SWORN to in my presence  
this 4<sup>th</sup> day of March, 2020.

  
DANETA WOLLMANN  
U.S. MAGISTRATE JUDGE

**ATTACHMENT A**

**Property to Be Searched**

This warrant applies to information associated with the following Facebook user IDs that are stored at premises owned, maintained, controlled, or operated by Facebook Inc., a company headquartered in Menlo Park, California:

- Karl.koster.75;
- ESP User ID: 100002462616167;
- Profile URL: <http://www.facebook.com/karl.koster.75>



**ATTACHMENT B**

**Particular Things to be Seized**

**I. Information to be disclosed by Facebook**

To the extent that the information described in Attachment A is within the possession, custody, or control of Facebook Inc. ("Facebook"), including any messages, records, files, logs, or information that have been deleted but are still available to Facebook, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Facebook is required to disclose the following information to the government for each user ID listed in Attachment A:

All contact and personal identifying information, including for Facebook user IDs and regarding the following account:

Karl.koster.75;

ESP User ID: 100002462616167;

Profile URL: <http://www.facebook.com/karl.koster.75>

- (a) including full name, user identification number, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.
- (b) All activity logs for the accounts and all other documents showing the user's posts and other Facebook activities;

- (c) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them;
- (d) All profile information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;
- (e) All other records of communications and messages made or received by the user, including all private messages, chat history, video calling history, and pending "Friend" requests;
- (f) All "check ins" and other location information;
- (g) All IP logs, including all records of the IP addresses that logged into the accounts;
- (h) All records of the accounts' usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked";
- (i) All information about the Facebook pages that the accounts are or were a "fan" of;
- (j) All past and present lists of friends created by the accounts;
- (k) All records of Facebook searches performed by the accounts;

- (l) All information about the users' access and use of Facebook Marketplace;
- (m) The types of service utilized by the user;
- (n) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);
- (o) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the accounts;
- (p) All records pertaining to communications between Facebook and any person regarding the user or the user's Facebook accounts, including contacts with support services and records of actions taken.

## **II. Information to be seized by the government**

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. §§ 2251, 2252, and 2252A, from January 1, 2019, to present, including, for the user ID identified on Attachment A.

## **III. Information Regarding Search Warrant Compliance by Facebook:**

Facebook shall disclose responsive data, if any, by sending to:

Det. Elliott Harding  
1444 Fountain Plaza Drive  
Rapid City, SD 57702  
(605) 394-4134  
Elliott.Harding@rcgov.org

Facebook shall use the United States Postal Service or another courier service to disclose the responsive data, notwithstanding 18 U.S.C. § 2252, 2252A or similar statute or code.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS  
RECORDS PURSUANT TO FEDERAL RULE OF EVIDENCE  
902(11)&(13)**

I, \_\_\_\_\_, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Facebook, and my official title is \_\_\_\_\_. I am a custodian of records for Facebook. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Facebook, and that I am the custodian of the attached records consisting of \_\_\_\_\_ (pages/CDs/kilobytes). I further state that:

- a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;
- b. such records were kept in the ordinary course of a regularly conducted business activity of Facebook; and
- c. such records were made by Facebook as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

\_\_\_\_\_  
Date

\_\_\_\_\_  
Signature

# UNITED STATES DISTRICT COURT

for the  
District of South Dakota

In the Matter of the Search of:  
INFORMATION ASSOCIATED WITH THE  
FOLLOWING FACEBOOK USER:  
Karl.koster.75; ESP User ID:  
100002462616167  
Profile URL:  
<http://www.facebook.com/karl.koster.75>  
THAT IS STORED AT PREMISES  
CONTROLLED BY FACEBOOK INC.

Case No. 5:20-mj-43

## SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the District of South Dakota (identify the person or describe the property to be searched and give its location):

See **ATTACHMENT A**, attached hereto and incorporated by reference

I find that the affidavit, or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

Evidence of a crime in violation of 18 U.S.C. §§ 2251, 2252, 2252A, as described in **ATTACHMENT B**, attached hereto and incorporated by reference.

I find that the affidavit, or any recorded testimony, establishes probable cause to search and seize the person or property.

**YOU ARE COMMANDED** to execute this warrant on or before March 18, 2020 (not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Daneta Wollmann.  
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for \_\_\_\_\_ days (not to exceed 30). ☐ until, the facts justifying, the later specific date of \_\_\_\_\_.

☐ I find that good cause has been established to authorize the officer executing this warrant to not provide notice prior to the execution of the search warrant, i.e., "no knock".

Date and time issued: 3-4-2020 9:30am

  
Judge's signature

City and state: Rapid City, SD

Daneta Wollmann, U.S. Magistrate  
Printed name and title

cc AUSA Collins and Agent - slt



## Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: \_\_\_\_\_

Executing officer's signature

---

Printed name and title